Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

  - **GNU GNU ChBg simplify_path() Buffer Overflow (Updated)**
  - **GNU CUPS HPGL ParseCommand() Buffer Overflow (Updated)**
  - **GNU CUPS lppasswd Denial of Service (Updated)**
  - **GNU Xpdf Buffer Overflow in doImage() (Updated)**
  - **Hewlett-Packard HP-UX SAM Privilege Escalation Vulnerability (Updated)**
  - IBM AIX NIS Client Remote Code Execution
  - IBM AIX chdev Format String
  - IBM AIX auditselect Format String
  - **Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow (Updated)**
  - Jim Faulkner Newspost Remote Buffer Overflow
  - KDE Konqueror IDN Implementation URL Spoof
  - **KDE kio_ftp FTP Command Injection Vulnerability (Updated)**
  - **KDE Konqueror Window Injection (Updated)**
  - **KDE Konqueror Java Sandbox Vulnerabilities (Updated)**
  - LOGICNOW PerlDesk 'view' Parameter Input Validation
  - Matt Wright WWWBoard Password Database Access Controls
  - Mike Neuman OSH Command Line Argument Buffer Overflow
  - Multiple Vendors Clam Anti-Virus ClamAV Remote Denial of Service
  - Multiple Vendors ht://Dig Cross-Site Scripting
  - Multiple Vendors Evolution Camel-Lock-Helper Application Remote Buffer Overflow (Updated)
  - **Multiple Vendors Squid Proxy Malformed HTTP Headers (Updated)**
  - **Multiple Vendors Zlib Compression Library Remote Denial of Service (Updated)**
  - **Multiple Vendors HylaFAX Remote Access Bypass (Updated)**
  - Multiple Vendors Perl SuidPerl Multiple Vulnerabilities
  - Multiple Vendors Linux Kernel NTFS File System Denial of Service
  - **Multiple Vendors ncpfs: ncplogin and ncpmap Buffer Overflow (Updated)**
  - **Multiple Vendors Samba smbd Security Descriptor (Updated)**
  - **Multiple Vendors Squid NTLM fakeauth_auth Helper Remote Denial of Service (Updated)**
  - Multiple Vendors Postfix IPv6 Security Bypass
  - **NetaTalk Insecure Temporary File Creation (Updated)**
  - newsgrab Directory Permission
  - OmniWeb IDN Implementation URL Spoof
  - **OpenSSL Insecure Temporary File Creation (Updated)**
  - **Petr Vandrovec ncpfs Access Control & Buffer Overflow (Updated)**
  - **PHPGroupware phpMyAdmin Two Vulnerabilities (Updated)**
  - **PHPMyAdmin Multiple Remote Cross-Site Scripting (Updated)**
  - **ProZilla Multiple Remote Buffer Overflow (Updated)**
  - **SCO UnixWare Mountd Remote Denial of Service (Updated)**
  - **Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow (Updated)**
  - SquirrelMail 'viewcert.php' Remote Code Execution
  - **SquirrelMail Vacation Plugin 'FTPFile' Input Validation (Updated)**
  - SquirrelMail Remote Code Execution
  - SuSE Linux Open-Xchange Path Traversal
  - **Todd Miller Sudo Restricted Command Execution BypasS (Updated)**
  - **University Of Washington IMAP Server CRAM-MD5 Remote Authentication Bypass (Updated)**
  - **Vim Insecure Temporary File Creation (Updated)**
  - **Yukihiro Matsumoto Ruby CGI Session Management Unsafe Temporary File (Updated)**
  - Yusuf Motiwala Newsfetch SScanf Remote Buffer Overflow
- Multiple Operating Systems
  - BXCP 'show' Local File Inclusion

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
DelphiTurk CodeBank 3.1 & prior	A vulnerability exists because username and passwords are stored in the Registry, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	DelphiTurk CodeBank Password Disclosure	Medium	SecurityTracker Alert, 1013093, February 7, 2005
EternalLines.com Eternal Lines Web Server 1.0	A remote Denial of Service vulnerability exists when a malicious user submits approximately 70 simultaneous connections to the target web server from the same originating host. No workaround or patch available at time of publishing. **An exploit script has been published.**	Eternal Lines Web Server Remote Denial of Service	Low	GSSIT Advisory, January 31, 2005 **SecurityFocus, February 1, 2005**
Foxmail Email Server 2.0	A buffer overflow vulnerability in the 'Mail From:' command due to a boundary error, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Foxmail 'MAIL FROM:' Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA14145, February 8, 2005
IceWarp Web Mail 5.3	Multiple vulnerabilities exist: a vulnerability exists when accessing 'calendar_d.html,' 'calendar_m.html,' 'calendar_w.html,' and 'calendar_y.html' directly with a valid session ID in the 'id' parameter, which could let a remote malicious user obtain sensitive information; a vulnerability exists due to weak encryption of user credentials in the 'users.cfg,' 'settings.cfg,' 'user.dat,' and 'users.dat' files, which could let a malicious user obtain sensitive information; and multiple Cross-Site Scripting and HTML injection vulnerabilities exist which could let a remote malicious user execute arbitrary HTML and script code. **Upgrade available at: http://www.icewarp.com/downloads/webmail.html?PHPSESSID=363e38e9f350cceda950cc146f67196f** There is no exploit code required; however, Proofs of Concept exploits have been published.	IceWarp Web Mail Multiple Remote Vulnerabilities	Medium/High (High if arbitrary code can be executed)	ShineShadow Security Report, January 29, 2005 **SecurityFocus, February 3, 2005**
Microsoft Internet Explorer 6.0, SP1	A Cross-Zone Scripting vulnerability exists when using the 'AddChannel' method to add a channel, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer AddChannel Cross-Zone Scripting	High	GreyHats Security Group, February 2, 2005

Microsoft Windows Media Player 9 Series, Windows Messenger 5.0, MSN Messenger 6.1, 6.2	Several vulnerabilities exist: a vulnerability exists in Media Player due to a failure to properly handle PNG files that contain excessive width or height values, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Windows and MSN Messenger due to a failure to properly handle corrupt or malformed PNG files, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-009.mspx Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Media Player & Windows/MSN Messenger PNG Processing CVE Names: CAN-2004-1244 CAN-2004-0597	High	Microsoft Security Bulletin, MS05-009, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#259890
Microsoft **Windows 2000 SP 3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems**	A vulnerability exists in the DHTML Edit ActiveX control, which could let a remote malicious user inject arbitrary scripting code into a different window on the target user's system. **Patches available at:** **http://www.microsoft.com/technet/security/bulletin/MS05-013.msp** A Proof of Concept exploit has been published.	Microsoft Internet Explorer DHTML Edit Control Script CVE Name: CAN-2004-1319	High	Bugtraq, December 15, 2004 **Microsoft Security Bulletin, MS05-013, February 8, 2005** **US-CERT Technical Cyber Security Alert TA05-039A** **US-CERT Cyber Security Alert SA05-039A** **US-CERT Vulnerability Note VU#356600**
Microsoft Windows 2000 SP3 &SP4, Windows XP SP1 & SP2, XP 64-Bit Edition SP1, XP 64-Bit Edition Version 2003, Windows Server 2003, Server 2003 for Itanium-based Systems, Windows 98, SE, ME	A vulnerability exists due to the way Drag-and-Drop events are handled, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-008.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Drag and Drop CVE Name: CAN-2005-0053	High	Microsoft Security Bulletin, MS05-008, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT

				Vulnerability Note VU#698835
Microsoft ASP.NET 1.x	A vulnerability exists which can be exploited by malicious people to bypass certain security restrictions. The vulnerability is caused due to a canonicalization error within the .NET authentication schema. Apply ASP.NET ValidatePath module: http://www.microsoft.com/downloads/details.aspx?FamilyId=DA77B852-DFA0-4631-AAF9-8BCC6C743026 **Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-004.mspx** A Proof of Concept exploit has been published.	Microsoft ASP.NET Canonicalization CVE Name: CAN-2004-0847	Medium	Microsoft, October 7, 2004 **Microsoft Security Bulletin, MS05-004, February 8, 2005** **US-CERT Technical Cyber Security Alert TA05-039A** **US-CERT Vulnerability Note VU#283646**
Microsoft Office XP SP2 & SP3, Project 2002, Visio 2002, Works Suite 2002, 2003, 2004	A buffer overflow vulnerability exists due to a boundary error in the process that passes URL file locations to Office, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-005.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Office URL File Location Handling Buffer Overflow CVE Name: CAN-2004-0848	High	Microsoft Security Bulletin, MS05-005, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#416001
Microsoft Windows 2000 SP3 & SP4, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	A buffer overflow vulnerability exists when handling Server Message Block (SMB) traffic, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-011.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows SMB Buffer Overflow CVE Name: CAN-2005-0045	High	Microsoft Security Bulletin, MS05-011, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note

				VU#652537
Microsoft Windows 2000 SP3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	Multiple vulnerabilities exist: a vulnerability exists due to insufficient validation of drag and drop events from the Internet zone to local resources, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to the way certain encoded URLs are parsed, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the validation of URLs in CDF (Channel Definition Format) files, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to an input validation error in the 'createControlRange()' javascript function, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient cross-zone restrictions; a vulnerability exists due to the way web sites are handled inside the 'Temporary Internet Files' folder; and a vulnerability exists in the 'codebase' attribute of the 'object' tag due to a parsing error. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-014.mspx Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Internet Explorer Vulnerabilities CVE Names: CAN-2005-0053 CAN-2005-0054 CAN-2005-0055 CAN-2005-0056	High	Microsoft Security Bulletin, MS05-014, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Notes VU#580299, VU#823971 VU#843771 VU#698835
Microsoft Windows 2000 SP3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	Two vulnerabilities exist: a vulnerability exists in OLE due to the way input validation is handled, which could let a remote malicious user execute arbitrary code; and a vulnerability exists when processing COM structured storage files, which could let a remote malicious execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-012.mspx Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Windows OLE / COM Remote Code Execution CVE Names: CAN-2005-0044 CAN-2005-0047	High	Microsoft Security Bulletin, MS05-012, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Notes VU#597889, VU#927889
Microsoft Windows 2000 SP3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1, (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for	A buffer overflow vulnerability exists in the Hyperlink Object Library when handling hyperlinks, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-015.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Hyperlink Object Library Buffer Overflow CVE Name: CAN-2005-0057	High	Microsoft Security Bulletin, MS05-015, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A

Itanium-based Systems				US-CERT Vulnerability Note VU#820427
Microsoft Windows NT Server 4.0 SP6a, Windows NT Server 4.0 Terminal Server Edition SP6a, Windows 2000 Server SP3 & SP4, Windows 2003, Windows 2003 for Itanium-based Systems	A buffer overflow vulnerability exists in the License Logging service due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-010.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows License Logging Service Buffer Overflow CVE Name: CAN-2005-0050	Low/High (High if arbitrary code can be executed)	Microsoft Security Bulletin, MS05-010, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#130433
Microsoft Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange Server 2003	A remote code execution vulnerability exists in the Windows Server 2003 SMTP component due to the way Domain Name System (DNS) lookups are handled. A malicious user could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution. The vulnerability also exists in the Microsoft Exchange Server 2003 Routing Engine component when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx Bulletin updated to clarify restart requirement for Windows Server 2003 and Windows XP 64-Bit. **Bulletin updated to advise of the availability of an update for Exchange 2000 Server.** Currently we are not aware of any exploits for this vulnerability.	Microsoft SMTP Remote Code Execution CVE Name: CAN-2004-0840	High	Microsoft Security Bulletin, MS04-035, October 12, 2004 US-CERT Cyber Security Alert, SA04-286A US-CERT Vulnerability Note VU#394792 Microsoft Security Bulletin MS04-035, November 9, 2004 **Microsoft Security Bulletin MS04-035 V2.0 February 8, 2005**
Microsoft Windows SharePoint Services for Windows Server 2003, SharePoint Team Services	A Cross-Site Scripting and spoofing vulnerability exists due to insufficient validation of input provided to a HTML redirection query before returning it to a user's browser, which could let a remote malicious user execute arbitrary HTML and script code and spoof web browser content. Patches available at: http://www.microsoft.com/technet/	Microsoft Windows SharePoint Services Cross-Site Scripting & Spoofing	High	Microsoft Security Bulletin, MS05-006, February 8, 2005 US-CERT

from Microsoft	security/bulletin/MS05-006.mspx Currently we are not aware of any exploits for this vulnerability.	CVE Name: CAN-2005-0049		Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#340409
Microsoft Windows XP SP1 & SP2, XP 64-Bit Edition SP1	A vulnerability exists in the authentication validation process when using named pipe connections, which could let a remote malicious user obtain sensitive information. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-007.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows XP Named Pipe Information Disclosure CVE Name: CAN-2005-0051	Medium	Microsoft Security Bulletin, MS05-007, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#939074
Netscape Netscape 7.x	A vulnerability exists when processing International Domain Names (IDNs), which could let a remote malicious user spoof web sites. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Netscape IDN Implementation URL Spoof	Medium	Secunia Advisory, SA14165, February 7, 2005
People Can Fly Painkiller 1.35 & prior	A buffer overflow vulnerability exists due to insufficient bounds checking in the Gamespy CD-key hash, which could let a remote malicious user cause a Denial of Service. Update available at: www.painkillergame.com/ A Proof of Concept exploit has been published.	Painkiller Buffer Overflow Remote Denial of Service	Low	Securiteam, February 3, 2005
Piotr Kowalski LANChat Pro Revival1.666c	A remote Denial of Service vulnerability exists due to a failure to process unexpected data. No workaround or patch available at time of publishing. An exploit script has been published.	Piotr Kowalski LANChat Pro Remote Denial of Service	Low	SecurityTracker Alert ID, 1013082, February 3, 2005
Qualcomm Eudora 6.2.0 & prior	Several vulnerabilities exist when viewing emails and handling stationary and mailbox files due to unspecified errors, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.eudora.com/products/ Currently we are not aware of any exploits for these	Eudora E-mail, Stationary/Mailbox Files Remote Code Execution	High	NGSSoftware Advisory, February 2, 2005

	vulnerabilities.			
RaidenHTTPD TEAM RaidenHTTPD 1.1.27	A Directory Traversal vulnerability when handling HTTP requests that contain relative pathnames due to an input validation error, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://www.raidenhttpd.com/en/download.html A Proof of Concept exploit has been published.	RaidenHTTPD Directory Traversal	Medium	Securiteam, February 6, 2005
RARLAB WinRar 3.0 .0, 3.10, beta 5, beta 3, 3.11, 3.20, 3.40-3.42	A Directory Traversal vulnerability exists when attempting to decompress a file by right clicking, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	RARLAB WinRAR Directory Traversal	Medium	7a69ezine Advisories, 7a69Adv#21, February 2, 2005
Real Networks RealPlayer 10.5 v6.0.12.1056, v6.0.12.1053, v6.0.12.1040, 10.5 Beta v6.0.12.1016, 10.5	A vulnerability exists due to insufficient enforcement of security zones, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	RealPlayer Security Zone Bypass	High	Bugtraq, February 1, 2005
Savant Savant Webserver 3.1	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Exploit scripts have been published.	Savant Web Server Remote Buffer Overflow	High	Securiteam, February 2, 2005
Software602 602LAN SUITE 2004	A vulnerability exists due to improper validation of user-supplied filenames before uploading files as e-mail attachments, which could let a remote malicious user execute arbitrary code. Update available at: http://www.software602.com/download/ Currently we are not aware of any exploits for this vulnerability.	602LAN SUITE Input Validation	High	SIG^2 Vulnerability Research Advisory, February 8, 2005
ZipGenius ZipGenius Standard Edition 5.5, Suite Edition 5.5	Multiple Directory Traversal vulnerabilities exist due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://web.rossoalice.it/zipgenius/zg6/zg6sui_b5.exe There is no exploit code required.	ZipGenius Multiple Directory Traversal Vulnerabilities	Medium	7a69ezine Advisories, 7a69Adv#19 & 20, February 2, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source

Alexander Barton ngIRCd 0.6, 0.6.1, 0.7, 0.7.1, 0.7.5-0.7.7, 0.8-0.8.2	A format string vulnerability exists in 'log.c' due to insufficient sanitization of the 'Log_Resolver()' function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Alexander Barton ngIRCd Remote Format String	High	No System Group, Adv #11, February 3, 2005
Apple Safari 1.2.4 v125.12	An input validation vulnerability exists because the HTTP 'Content-type' header value is ignored by the web server, which could let a remote malicious user modify system information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apple Safari Input Validation	Medium	SecurityTracker Alert ID 1013087, February 5, 2
Apple Safari 1.2.5	A vulnerability exists when processing International Domain Names (IDNs), which could let a remote malicious user spoof web sites. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apple Safari IDN Implementation URL Spoof	Medium	Secunia Advisory, SA14164, February 7, 2
ARJ Software Inc. UNARJ 2.62-2.65	A buffer overflow vulnerability exists due to insufficient bounds checking on user-supplied strings, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-29.xml SUSE: http://www.suse.de/de/security/2004_03_sr.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-007.html Debian: http://security.debian.org/pool/updates/non-free/u/unarj/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-022_RHSA-2005-007.pdf **Fedora Legacy:** **http://download.fedoralegacy.org/redhat/** **http://download.fedoralegacy.org/fedora/1/updates/** Currently we are not aware of any exploits for this vulnerability.	ARJ Software UNARJ Remote Buffer Overflow CVE Name: CAN-2004-0947	High	SecurityTracker Alert I, 1012194, November 11 Gentoo Linux Security Advisory, GLSA 20041 November 19, 2004 SUSE Security Summa Report SUSE-SR:2004 December 7, 2004 Fedora Update Notifica FEDORA-2004-414, De 11, 2004 RedHat Security Adviso RHSA-2005:007-05, Ja 12, 2005 Debian Security Adviso 652-1, January 21, 200 Avaya Security Advisor ASA-2005-022, Januar 2005 **Fedora Legacy Updat Advisory, FLSA:2272, February 1, 2005**

FireHOL FireHOL 1.214	A vulnerability exists due to the insecure creation of various temporary files, which could let a malicious user overwrite arbitrary files. Update available at: http://firehol.sourceforge.net/ **Gentoo: http://security.gentoo.org/glsa/glsa-200502-01.xml** There is no exploit required	FireHOL Insecure Local Temporary File Creation	Medium	Secunia Advisory, SA1 January 25, 2005 **Gentoo Linux Securit Advisory, GLSA 2005 February 1, 2005**
Freedesktop.org D-BUS 0.23 & prior	A vulnerability exists in 'bus/policy.c' due to insufficient restriction of connections, which could let a malicious user hijack a session bus. Patch available at: https://bugs.freedesktop.org/show_bug.cgi?id=2436 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ There is no exploit code required.	D-BUS Session Hijack CVE Name: CAN-2005-0201	Medium	SecurityTracker Alert ID,1013075, February 3
FreeRADIUS Server Project FreeRADIUS 0.2-0.5, 0.8, 0.8.1, 0.9-0.9.3. 1.0	A remote Denial of Service vulnerability exists in 'radius.c' and 'eap_tls.c' due to a failure to handle malformed packets. Upgrades available at: ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-29.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-609.html **Fedora Legacy: http://download.fedoralegacy.org/fedora/1/updates/** There is no exploit code required.	FreeRADIUS Access-Request Denial of Service CVE Names: CAN-2004-0938 CAN-2004-0960 CAN-2004-0961	Low	Gentoo Linux Security Advisory, GLSA 20040 September 22, 2004 US-CERT Vulnerability VU#541574, October 1 Fedora Update Notifica FEDORA-2004-355, Oc 28, 2004 RedHat Security Adviso RHSA-2004:609-06, No 12, 2004 **Fedora Legacy Updat Advisory, FLSA:2187, February 1, 2005** **US-CERT Vulnerabilit VU#541574**
Frox Frox 0.7.16, 0.7.17	A vulnerability exists in 'config.c' due to improper parsing of Deny ACLs in the 'parse_match()' function, which could let a remote malicious user bypass security restrictions. Update available at: http://frox.sourceforge.net/download/ Currently we are not aware of any exploits for this vulnerability.	Frox Deny ACL Parsing	Medium	Secunia Advisory, SA14182, February 8, 2
Gallery Project Gallery 1.4 -pl1&pl2, 1.4, 1.4.1, 1.4.2,	A Cross-Site Scripting vulnerability exists in several files, including 'view_photo.php,' 'index.php,' and 'init.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and	Gallery Cross-Site Scripting	High	Gentoo Linux Security Advisory, GLSA 20041 November 6, 2004

1.4.3 -pl1 & pl2; Gentoo Linux	script code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=7130 Gentoo: http://security.gentoo.org/glsa/glsa-200411-10.xml Debian: http://security.debian.org/pool/updates/main/g/gallery/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-45.xml** **It is reported that the fixes released by the vendor to address this issue are ineffective. Gallery 1.4.4-pl2 is still considered vulnerable to cross-site scripting attacks. The fixes are being removed.** There is no exploit code required.	**CVE Name:** **CAN-2004-1106**		Debian Security Adviso 642-1, January 17, 200 **Gentoo Linux Securit Advisory, GLSA 2005 January 30, 2005** **SecurityFocus, Febru 2005**
Glyph and Cog XPDF prior to 3.00pl3	A buffer overflow vulnerability exists in ' 'xpdf/Decrypt.cc' due to a boundary error in the 'Decrypt::makeFileKey2' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.foolabs.com/xpdf/download.html Patch available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch Debian: http://security.debian.org/pool/updates/main/c/cupsys/ http://security.debian.org/pool/updates/main/x/xpdf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/ KDE: ftp://ftp.kde.org/pub/kde/security_patches Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow CVE Name: CAN-2005-0064	High	iDEFENSE Security Ad January 18, 2005 Conectiva Linux Securi Announcement, CLA-2 January 25, 2005 Mandrakelinux Security Advisories, MDKSA-2005:016-021, 26, 2005 SUSE Security Summa Report, SUSE-SR:2005 January 26, 2005 **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**

GNU Emacs prior to 21.4.17	A format string vulnerability exists in 'movemail.c,' which could let a remote malicious user execute arbitrary code. Update available at: ftp://ftp.xemacs.org/pub/xemacs/xemacs-21.4 Currently we are not aware of any exploits for this vulnerability.	Emacs Format String CVE Name: CAN-2005-0100	High	SecurityTracker Alert, 1 February 7, 2005
GNU Midnight Commander Project Midnight Commander 4.x	Multiple vulnerabilities exist due to various design and boundary condition errors, which could let a remote malicious user cause a Denial of Service, obtain elevated privileges, or execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	Midnight Commander Multiple Vulnerabilities CVE Names: CAN-2004-1004 CAN-2004-1005 CAN-2004-1009 CAN-2004-1090 CAN-2004-1091 CAN-2004-1092 CAN-2004-1093 CAN-2004-1174 CAN-2004-1175 CAN-2004-1176	Low/ Medium/ High (Low if a DoS; Medium is elevated privileges can be obtained; and High if arbitrary code can be executed)	SecurityTracker Alert, 1 January 14, 2005 **SUSE Security Summ** **Report, SUSE-SR:200** **February 4, 2005**
GNU ChBg 1.5	A vulnerability was reported in ChBg. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ChBg scenario file that, when processed by the target user with ChBg, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the simplify_path() function in 'config.c.' FreeBSD is not affected because PATH_MAX is set to 1024, preventing the buffer overflow. Debian: http://security.debian.org/pool/updates/main/c/chbg/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** A Proof of Concept exploit script has been published.	GNU ChBg simplify_path() Buffer Overflow CVE Name: CAN-2004-1264	High	Secunia Advisory ID, S December 17, 2004 Debian Security Adviso 644-1, January 18, 200 **Mandrakelinux Securi** **Update Advisory,** **MDKSA-2005:027, Fel** **2005**
GNU CUPS 1.1.22	A vulnerability was reported in CUPS in the processing of HPGL files. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted HPGL file that, when printed by the target user with CUPS, will execute arbitrary code on the target user's system. The code will run with the privileges of the 'lp' user. The buffer overflow resides in the ParseCommand() function in 'hpgl-input.c.' Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/	GNU CUPS HPGL ParseCommand() Buffer Overflow **CVE Name:** **CAN-2004-1267**	High	CUPS Advisory STR #1 December 16, 2004 Mandrakelinux Security Advisory, MDKSA-2005 January 17, 2005 SGI Security Advisory, 20050101-01-U, Janua 2005 **SUSE Security Summ** **Report, SUSE-SR:200** **February 4, 2005**

	Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: http://www.sgi.com/support/security/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit script has been published.			
GNU CUPS lppasswd 1.1.22	A vulnerability was reported in the CUPS lppasswd utility. A local malicious user can truncate or modify certain files and cause Denial of Service conditions on the target system. There are flaws in the way that lppasswd edits the '/usr/local/etc/cups/passwd' file. Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-013.html **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **SGI:** **http://www.sgi.com/support/security/** A Proof of Concept exploit has been published.	GNU CUPS lppasswd Denial of Service CVE Name: CAN-2004-1268	Low	SecurityTracker Alert ID 1012602, December 16 **Mandrakelinux Securi Update Advisory, MDKSA-2005:008, Jan 17, 2005** **SGI Security Advisory 20050101-01-U, Janua 2005**
GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Mandrakesoft (update for koffice):	GNU Xpdf Buffer Overflow in doImage() CVE Name: CAN-2004-1125	High	iDEFENSE Security Ad 12.21.04 KDE Security Advisory, December 23, 2004 Mandrakesoft, MDKSA-2004:161,162, 166, December 29, 200 Fedora Update Notifica FEDORA-2004-585, Ja 2005 Gentoo Linux Security Advisory, GLSA 20050 January 10, 2005 Conectiva Linux Securi Announcement, CLA-2 January 25, 2005 SUSE Security Summa Report, SUSE-SR:2005 January 26, 2005 Avaya Security Advisor ASA-2005-027, Januar 2005

	http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:165 Mandrakesoft (update for kdegraphics): http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:163 Mandrakesoft (update for gpdf): http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:162 Mandrakesoft (update for xpdf): http://www.mandrakesoft.com/security /advisories?name=MDKSA-2004:161 Mandrakesoft (update for tetex): http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:166 Debian: http://www.debian.org/security/2004/dsa-619 Fedora (update for tetex): http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/ glsa-200501-13.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ SGI: http://support.sgi.com/browse_ request/linux_patches_by_os Conectiva: ftp://atualizacoes.conectiva.com.br/ **SuSE: ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.			**SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**
Hewlett-Packard HP-UX 11.x	A vulnerability exists which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to an unspecified error in SAM (System Administration Manager). Apply patches: http://www.itrc.hp.com/service/ patch/mainPage.do **Rev 2: Added B.11.04 patch** Currently we are not aware of any exploits for this vulnerability.	Hewlett-Packard HP-UX SAM Privilege Escalation Vulnerability	Medium	HP Advisory, SSRT469 December 22, 2004 **HP Security Bulletin, HPSBUX01104 Rev 2, February 1, 2004**
IBM AIX 5.3	A vulnerability exists in the NIS client, which could let a remote malicious user execute arbitrary code.	IBM AIX NIS Client Remote Code Execution	High	SecurityFocus, Februar 2005

	Patch available at: ftp://aix.software.ibm.com/aix/efixes/security/nis_efix.tar.Z Currently we are not aware of any exploits for this vulnerability.			
IBM AIX 5.1-5.3	A format string vulnerability exists in '/usr/sbin/chdev,' which could let a malicious user obtain root privileges. Updates available at: http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html Currently we are not aware of any exploits for this vulnerability.	IBM AIX chdev Format String	High	iDEFENSE Security Ad February 7, 2005
IBM AIX 5.2, 5.3	A format string vulnerability exists in auditselect, which could let a malicious user obtain root privileges. Updates available at: http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html Currently we are not aware of any exploits for this vulnerability.	IBM AIX auditselect Format String CVE Name: CAN-2005-0250	High	SecurityTracker Alert, 1 February 8, 2005
Info-ZIP Zip 2.3; Avaya CVLAN, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing	A buffer overflow vulnerability exists due to a boundary error when doing recursive compression of directories with 'zip,' which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zip/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE Red Hat: http://rhn.redhat.com/errata/RHSA-2004-634.html **Debian:** **http://www.debian.org/security/2005/dsa-624** TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-019_RHSA-2004-634.pdf **Fedora Legacy:**	Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow CVE Name: CAN-2004-1010	High	Bugtraq, November 3, 2 Ubuntu Security Notice USN-18-1, November 5 Fedora Update Notifica FEDORA-2004-399 & FEDORA-2004-400, No 8 & 9, 2004 Gentoo Linux Security Advisory, GLSA 20041 November 9, 2004 Mandrakelinux Security Advisory, MDKSA-2004 November 26, 2004 SUSE Security Summa Report, SUSE-SR:2004 December 7, 2004 Red Hat Advisory, RHSA-2004:634-08, De 16, 2004 Debian DSA-624-1, Jan 2005 Turbolinux Security Announcement, 200501 January 31, 2005 Avaya Security Advisor ASA-2005-019, Januar 200 **Fedora Legacy Updat Advisory, FLSA:2255, February 1, 2005**

	http://download.fedoralegacy.org/redhat/ **http://download.fedoralegacy.org/fedora/1/updates/** Currently we are not aware of any exploits for this vulnerability.			
Jim Faulkner Newspost 2.0, 2.1.1	A buffer overflow vulnerability exists in 'socket.c' in the the 'socket_getline()' function when handling NNTP server responses, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200502-05.xml A Proof of Concept exploit script has been published.	Newspost Remote Buffer Overflow CVE Name: CAN-2005-0101	High	Secunia Advisory, SA14092, February 1, 2 Gentoo Linux Security Advisory, GLSA 20050 February 3, 2004
KDE.org Konqueror 3.x	A vulnerability exists when processing International Domain Names (IDNs), which could let a remote malicious user spoof web sites. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	KDE Konqueror IDN Implementation URL Spoof	Medium	Secunia Advisory, SA14162, February 7, 2
KDE KDE 3.x, 2.x	A vulnerability exists in kio_ftp, which can be exploited by malicious people to conduct FTP command injection attacks. The vulnerability has been fixed in the CVS repository. Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:160 Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-18.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	KDE kio_ftp FTP Command Injection Vulnerability CVE Name: CAN-2004-1165	Medium	KDE Advisory Bug 958 December 26, 2004 Debian Security Adviso 631-1, January 10, 200 Gentoo Linux Security Advisory, GLSA 20050 January 11, 2005 Fedora Update Notifica FEDORA-2005-063 & 0 January 25, 2005 **SUSE Security Summ** **Report, SUSE-SR:200** **February 4, 2005**
KDE Konqueror 3.2.2-6	A vulnerability exists which can be exploited by malicious people to spoof the content of websites. A website can inject content into another site's window if the target name of the window is known. This can be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrakesoft:	KDE Konqueror Window Injection CVE Name: CAN-2004-1158	Medium	Secunia Advisory ID, S December 8, 2004 Secunia Advisory ID, S December 16, 2004 Mandrakesoft Security Advisory, MDKSA-2004 December 15, 2004 **SUSE Security Summ** **Report, SUSE-SR:200**

	http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:150 Gentoo: http://security.gentoo.org/glsa/ glsa-200412-16.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.			**February 4, 2005**
KDE Konqueror prior to 3.32	Two vulnerabilities exist in KDE Konqueror, which can be exploited by malicious people to compromise a user's system.The vulnerabilities are caused due to some errors in the restriction of certain Java classes accessible via applets and Javascript. This can be exploited by a malicious applet to bypass the sandbox restriction and read or write arbitrary files. Update to version 3.3.2: http://kde.org/download/ Apply patch for 3.2.3: ftp://ftp.kde.org/pub/kde/security patches/post-3.2.3-kdelibs-khtml-java.tar.bz2 Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:154 Gentoo: http://security.gentoo.org/glsa/glsa-200501-16.xml Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	KDE Konqueror Java Sandbox Vulnerabilities CVE Name: CAN-2004-1145	High	KDE Security Advisory, December 20, 2004 Mandrakesoft MDKSA-2004:154, Dec 22, 2004 US-CERT Vulnerability VU#420222, January 5 Gentoo Linux Security Advisory, GLSA 20050 January 11, 2005 Fedora Update Notifica FEDORA-2005-063 & 0 January 25, 2005 **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**
LOGICNOW PerlDesk 1.x	An input validation vulnerability exists in the 'kb.cgi' script due to insufficient validation of the 'view' parameter, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PerlDesk 'view' Parameter Input Validation	High	SecurityTracker Alert, 1 February 7, 2005
Matt Wright WWWBoard 2.0 Alpha 2.1, 2.0 Alpha 2	A vulnerability exists in the password database file due to insufficient access controls, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	WWWBoard Password Database Access Controls	Medium	SecurityFocus, Februar 2005

Mike Neuman osh 1.7	A buffer overflow vulnerability exists in 'main.c' due to insufficient bounds checking in the 'iopen()' function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Mike Neuman OSH Command Line Argument Buffer Overflow	High	Secunia Advisory, SA14159, February 8,
Multiple Vendors ClamAV 0.51-0.54, 0.60, 0.65, 0.67, 0.68 -1, 0.68, 0.70, 0.80 rc1-rc4, 0.80; MandrakeSoft Corporate Server 3.0 x86_64, 3.0. Linux Mandrake 10.1 X86_64, 10.1	A remote Denial of Service vulnerability exists due to an error in the handling of file information in corrupted ZIP files. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=300116 Gentoo: http://security.gentoo.org/glsa/glsa-200501-46.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	Clam Anti-Virus ClamAV Remote Denial of Service CVE Name: CAN-2005-0133	Low	SecurityFocus, January 2005 Mandrakelinux Security Advisory, MDKSA-2005 January 31, 2005 Gentoo Linux Security Advisory, GLSA 20050 January 31, 2005 SUSE Security Summa Report, SUSE-SR:2005 February 4, 2005
Multiple Vendors ht//Dig Group ht://Dig 3.1.5 -8, 3.1.5 -7, 3.1.5, 3.1.6, 3.2 .0, 3.2 0b2-0b6; SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, 9.0 x86_64, 9.1, 9.2	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from the 'config' parameter, which could let a remote malicious user execute arbitrary HTML and script code. SuSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required; however, a Proof of Concept exploit has been published.	ht://Dig Cross-Site Scripting CVE Name: CAN-2005-0085	High	SUSE Security Summa Report, SUSE-SR:2005 February 4, 2005
Multiple Vendors MandrakeSoft Corporate Server 3.0, x86_64, Linux Mandrake 10.0, AMD64, 10.1, X86_64;Novell Evolution 2.0.2l Ubuntu Linux 4.1 ppc, ia64, ia32; Ximian Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.4, 1.3.2 (beta)	A buffer overflow vulnerability exists in the main() function of the 'camel-lock-helper.c' source file, which could let a remote malicious user execute arbitrary code. Update available at: http://cvs.gnome.org/viewcvs/evolution/camel/camel-lock-helper.c?rev=1.7&hideattic=0&view=log Gentoo: http://security.gentoo.org/glsa/glsa-200501-35.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Evolution Camel-Lock-Helper Application Remote Buffer Overflow CVE Name: CAN-2005-0102	High	Gentoo Linux Security Advisory, GLSA 20050 January 25, 2005 Ubuntu Security Notice USN-69-1, January 25, Mandrakelinux Security Advisory, MDKSA-2005 January 27, 2005 **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**

Multiple Vendors SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, x86_64, 9.1, 9.2; Squid Web Proxy Cache 2.5 .STABLE3-STABLE7, 2.5 .STABLE1	A vulnerability exists due to a failure to handle malformed HTTP headers. The impact was not specified. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/ bugs/squid-2.5.STABLE7-oversize_reply_headers.patch Gentoo: http://security.gentoo.org/ glsa/glsa-200502-04.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	Squid Proxy Malformed HTTP Headers CVE Name: CAN-2005-0174	Not Specified	Gentoo Linux Security Advisory, GLSA 20050 February 2, 2005 SUSE Security Summa Report, SUSE-SR:2005 February 4, 2005 **US-CERT Vulnerabilit VU#768702** **US-CERT Vulnerabilit VU#823350**

Multiple Vendors
FileZilla Server 0.7, 0.7.1; OpenBSD -current, 3.5;
OpenPKG Current, 2.0, 2.1;
zlib 1.2.1
	A remote Denial of Service vulnerability during the decompression process due to a failure to handle malformed input.
	Gentoo:
	http://security.gentoo.org/glsa/ glsa-200408-26.xml
	FileZilla:
	http://sourceforge.net/project/showfiles. php?group_id=21558
	OpenBSD:
	ftp://ftp.openbsd.org/pub/OpenBSD/patches/ 3.5/common/017_libz.patch
	OpenPKG:
	ftp ftp.openpkg.org
	Trustix:
	ftp://ftp.trustix.org/pub/trustix/updates/
	SuSE:
	ftp://ftp.suse.com/pub/suse/
	Mandrake:
	http://www.mandrakesecure.net/ en/ftp.php
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	SCO:
	ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2004.17
	Fedora:
	http://download.fedora.redhat.com /pub/fedora/linux/core/updates/2/
	We are not aware of any exploits for this vulnerability.
		Zlib Compression Library Remote Denial of Service
		CVE Name:
		CAN-2004-0797
			Low	SecurityFocus, August
				SUSE Security Announ SUSE-SA:2004:029, September 2, 2004
				Mandrakelinux Security Advisory, MDKSA-2004 September 8, 2004
				Conectiva Linux Securi Announcement, CLA-2 September 13, 2004
				US-CERT Vulnerability VU#238678, October 1
				SCO Security Advisory SCOSA-2004.17, Octo 2004
				Conectiva Linux Securi Announcement, CLA-2 October 25, 2004
				Fedora Update Notific FEDORA-2005-095, Ja 28, 2005

Multiple Vendors Hylafax.org Hylafax 4.0 pl0-pl2, 4.0.2, 4.1, beta1-beta3, 4.1.1-4.1.3, 4.1.5-4.1.8; 4.2; MandrakeSoft Linux	A vulnerability exists because the username is incorrectly compared with an entry in the 'hosts.hfaxd' database, which could let a remote malicious user obtain unauthorized access. Patches available at: ftp://ftp.hylafax.org/source/hylafax-4.2.1.tar.gz	HylaFAX Remote Access Bypass CVE Name: CAN-2004-1182	Medium	SecurityTracker Alert, 1 January 12, 2005 **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**

Mandrake 10.0, AMD64, 10.1 X86_64, 10.1	Debian: http://security.debian.org/ pool/updates/main/h/hylafax/ Gentoo: http://security.gentoo.org/ glsa/glsa-200501-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit required.			
Multiple Vendors Larry Wall Perl 5.8, 5.8.1, 5.8.3, 5.8.4, 5.8.4 -1-5.8.4-5; Ubuntu Linux 4.1 ppc, ia64, ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PERLIO_DEBUG' SuidPerl environment variable, which could let a malicious user execute arbitrary code; and a vulnerability exists due to an error when handling debug message output, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/universe/p/perl/ Currently we are not aware of any exploits for these vulnerabilities.	Perl SuidPerl Multiple Vulnerabilities CVE Names: CAN-2005-0155 CAN-2005-0156	Medium/ High (High if arbitrary code can be executed)	Ubuntu Security Notice USN-72-1, February 2,
Multiple Vendors Linux Kernel 2.6.x	A Denial of Service vulnerability exists in 'fs/ntfs/debug.c' because kernel error messages are not properly limited. Update available at: http://kernel.org/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel NTFS File System Denial of Service	Low	Secunia Advisory, SA1 February 7, 2005
Multiple Vendors ncpfs 2.2.1 - 2.2.4	A buffer overflow exists that could lead to local execution of arbitrary code with elevated privileges. The vulnerability is in the handling of the '-T' option in the ncplogin and ncpmap utilities, which are both installed as SUID root by default. Gentoo: Update to 'net-fs/ncpfs-2.2.5' or later http://www.gentoo.org/security/en /glsa/glsa-200412-09.xml SUSE: Apply updated packages. Updated packages are available via YaST Online Update or the SUSE FTP site. **Mandrake:** **http://www.mandrakesecure.net/ en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors ncpfs: ncplogin and ncpmap Buffer Overflow CVE Name: CAN-2004-1079	High	Gentoo Linux Security Advisory, GLSA 20041 ncpfs, December 15, 2 Secunia SA13617, Dec 22, 2004 **Mandrakelinux Securi Update Advisory, MDKSA-2005:028, Feb 2005**

Multiple Vendors Samba 2.2.9, 3.0.8 and prior	An integer overflow vulnerability in all versions of Samba's smbd 0.8 could allow an remote malicious user to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges. Patches available at: http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch Red Hat: http://rhn.redhat.com/errata/RHSA-2004-670.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-13.xml Trustix: http://www.trustix.net/errata/2004/0066/ Red Hat (Updated): http://rhn.redhat.com/errata/RHSA-2004-670.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.novell.com/linux/security/advisories/2004_45_samba.html Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:158 Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-020.html **HP:** **http://software.hp.com** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Samba smbd Security Descriptor CVE Name: CAN-2004-1154	High	iDEFENSE Security Ad 12.16.04 Red Hat Advisory, RHSA-2004:670-10, De 16, 2004 Gentoo Security Adviso GLSA 200412-13 / San December 17, 2004 US-CERT, Vulnerability VU#226184, Decembe 2004 Trustix Secure Linux Ad #2004-0066, Decembe 2004 Red Hat, RHSA-2004:6 December 16, 2004 SUSE, SUSE-SA:2004 December 22, 2004 RedHat Security Adviso RHSA-2005:020-04, Ja 2005 Conectiva Linux Securi Announcement, CLA-2005:913,January **Turbolinux Security Announcement, Febru 2005** **HP Security Advisory HPSBUX01115, Febru 2005**
Multiple Vendors Squid 2.x; Gentoo Linux;Ubuntu Linux 4.1 ppc, ia64, ia32;Ubuntu Linux 4.1 ppc, ia64, ia32; Conectiva Linux 9.0, 10.0	A remote Denial of Service vulnerability exists in the NTLM fakeauth_auth helper when running under a high load or for a long period of time, and a specially crafted NTLM type 3 message is submitted. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-fakeauth_auth.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml	Squid NTLM fakeauth_auth Helper Remote Denial of Service CVE Name: CAN-2005-0096	Low	Secunia Advisory, SA13789, January 11, Gentoo Linux Security GLSA 200501-25, Janu 2005 Ubuntu Security Notice USN-67-1, January 20, Conectiva Linux Securi Announcement, CLA-2 January 26, 2005

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates** **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.			**Fedora Update Notific FEDORA-2005-105 & 1 February 1, 2005** **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**
Multiple Vendors SuSE Linux 8.0, i386, 8.1, 8.2, 9.0 x86_64, 9.0-9.2; Wietse Venema Postfix 2.1.3	A vulnerability exists because arbitrary mail with an IPv6 address can be sent to any MX host, which could let a remote malicious user bypass security. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/postfix/ SuSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required.	Postfix IPv6 Security Bypass	Medium	SUSE Security Summa Report, SUSE-SR:2005 February 4, 2005 Ubuntu Security Notice USN-74-2, February 4,
Netatalk Netatalk Open Source Apple File Share Protocol Suite 1.5 pre6, 1.6.1, 1.6.4	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-25.xml Mandrake: http://www.mandrakesoft.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	NetaTalk Insecure Temporary File Creation CVE Name: CAN-2004-0974	Medium	Trustix Secure Linux Bu Advisory, TSL-2004-00 September 30, 2004 Gentoo Linux Security GLSA 200410-25, Octo 2004 Mandrakelinux Security Advisory, MDKSA-2004 November 2, 2004 Fedora Update Notifica FEDORA-2004-505 & 5 December 6, 2004 **Turbolinux Security Announcement, 2005 January 31, 2005**

Newsgrab Newsgrab prior to 0.5.0pre4	Two vulnerabilities exist: a vulnerability exists in the 'newsgrab.pl' file due to the insecure creation of downloaded files in the output directory, which could let a remote malicious user overwrite arbitrary files; and a Directory Traversal vulnerability exists due to insufficient sanitization of input from newsgroups messages, which could let a remote malicious user place attachments in arbitrary locations. Update available at: http://sourceforge.net/project/showfiles.php?group_id=52048 A Proof of Concept exploit has been published.	newsgrab Directory Permissions CVE Names: CAN-2005-0153 CAN-2005-0154	Medium	Secunia Advisory, SA14083, February 3, 2
Omni Group OmniWeb 5.x	A vulnerability exists when processing International Domain Names (IDNs), which could let a remote malicious user spoof web sites. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	OmniWeb IDN Implementation URL Spoof	Medium	Secunia Advisory, SA1 February 7, 2005
OpenSSL Project OpenSSL 0.9.6, 0.9.6 a-0.9.6 m, 0.9.7c	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/openssl/ Debian: http://www.debian.org/security/2004/dsa-603 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:147 **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	OpenSSL Insecure Temporary File Creation CVE Name: CAN-2004-0975	Medium	Trustix Secure Linux Bu Advisory, TSL-2004-00 September 30, 2004 Gentoo Linux Security Advisory, GLSA 20041 November 8, 2004 Ubuntu Security Notice USN-24-1, November 1 Debian Security Adviso DSA-603-1, December Mandrakesoft Security Advisory, MDKSA-2004 December 6, 2004 **Turbolinux Security Announcement, 2005 January 31, 2005**

Petr Vandrovec ncpfs prior to 2.2.6	Two vulnerabilities exist: a vulnerability exists in 'ncpfs-2.2.0.18/lib/ncplib.c' due to improper access control in the 'ncp_fopen_nwc()' function, which could let a malicious user obtain unauthorized access; and a buffer overflow vulnerability exists in 'ncpfs-2.2.5/sutil/ncplogin.c' due to insufficient validation of the 'opt_set_volume_after_parsing_all_options()' function, which could let a malicious user execute arbitrary code. Update available at: ftp://platan.vc.cvut.cz/pub/linux/ncpfs/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-44.xml **Debian:** **http://www.debian.org/security/2005/dsa-665** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** An exploit script has been published.	Petr Vandrovec ncpfs Access Control & Buffer Overflow CVE Names: CAN-2005-0013 CAN-2005-0014	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID 1013019, January 28, 2 **Mandrakelinux Securi Update Advisory, MDKSA-2005:028, Feb 2005** **Debian Security Advis DSA-665-1, February 4** **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**
PHPGroupWare phpMyAdmin 2.4.0 up to 2.6.1-rc1	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system and by malicious users to disclose sensitive information.1) An input validation error in the handling of MySQL data allows injection of arbitrary shell commands. 2) Input passed to 'sql_localfile' is not properly sanitized in 'read_dump.php' before being used to disclose files. Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-19.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit has been published.	PHPGroupWare phpMyAdmin Two Vulnerabilities CVE Names: CAN-2004-1147 CAN-2004-1148	Medium/ High (High if arbitrary code can be executed)	Exaprobe, Security Adv December 13, 2004 **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**

phpMyAdmin Development Team phpMyAdmin 2.5 .0-2.5.7, 2.6 .0pl1&2	Multiple Cross-Site Scripting vulnerabilities exist: a vulnerability exists in 'config.inc.php' if the 'PmaAbsoluteUri' parameter is not set, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in 'read_dump.php' due to insufficient validation of the 'zero_rows' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists due to insufficient validation of inputs on the confirm page, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/ phpmyadmin/phpMyAdmin-2.6.0-pl3.tar.gz?download Gentoo: http://security.gentoo.org/ glsa/glsa-200411-36.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** Proofs of Concept exploits have been published.	PHPMyAdmin Multiple Remote Cross-Site Scripting	High	netVigilance Security A 5, November 19, 2004 Gentoo Linux Security Advisory, GLSA 20041 November 27, 2004 **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**
ProZIlla ProZilla Download Accelerator 1.0 x, 1.3.0-1.3.4, 1.3.5.2, 1.3.5 .1, 1.3.5, 1.3.6	Multiple buffer overflow vulnerabilities exist due to boundary errors in the communication handling, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200411-31.xml **Debian:** **http://security.debian.org/pool /updates/main/p/prozilla/** Exploit scripts have been published.	ProZilla Multiple Remote Buffer Overflow **CVE Name:** **CAN-2004-1120**	High	Secunia Advisory, SA13294, November 2 **Debian Security Advis DSA 663-1, February**
SCO Unixware 7.1.1, 7.1.3, 7.1.4; **Avaya Intuity Audix R5**	A remote Denial of Service vulnerability exists when the 'mountd' service is registered in 'inetd.conf.' Patches available at: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2005.1/erg712731.711.pkg.Z **Avaya:** **http://support.avaya.com/japple/css/ japple?temp.groupID=128450&temp. selectedFamily=128451&temp.selected Product=154235&temp.selectedBucket= 126655&temp.feedbackState=askFor Feedback&temp.documentID=215716& PAGE=avaya.css.CSSLvl1Detail&execute Transaction=avaya.css.UsageUpdate()** There is no exploit required.	SCO UnixWare Mountd Remote Denial of Service CVE Name: CAN-2004-1039	Low	SCO Security Advisory SCOSA-2005.1, Janua 2005 **Avaya Security Advis ASA-2005-029, Februa 2005**
Squid-cache.org Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 .STABLE4&5, 2.4 .STABLE6&7, 2.4 .STABLE2, 2.4, 2.5	Two vulnerabilities exist: remote Denial of Service vulnerability exists in the Web Cache Communication Protocol (WCCP) functionality due to a failure to handle unexpected network data; and buffer overflow vulnerability exists in the 'gopherToHTML()' function due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code.	Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow CVE Names:	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA1 January 13, 2005 Debian Security Adviso 651-1, January 20, 200 Ubuntu Security Notice USN-67-1, January 20,

.STABLE3-7, 2.5 .STABLE1; Conectiva Linux 9.0, 10.0	Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-wccp_denial_of_service.patch http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-gopher_html_parsing.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml Debian: http://security.debian.org/pool/updates/main/s/squid/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates** **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit required.	CAN-2005-0094 CAN-2005-0095		Mandrakelinux Security Advisory, MDKSA-2005 January 25, 2005 Conectiva Linux Securi Announcement, CLA-2 January 26, 2005 **Fedora Update Notific FEDORA-2005-105 & 1 February 1, 2005** **SUSE Security Summ Report, SUSE-SR:200 February 4, 2005**
SquirrelMail Development Team SquirrelMail prior to 0.6	A vulnerability exists in the 'viewcert.php' script due to insufficient validation of the 'cert' parameter when passing data to an exec() call, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.squirrelmail.org/plugin_view.php?id=54 http://www.squirrelmail.org/plugin_download.php?id=54&rev=1141 Currently we are not aware of any exploits for this vulnerability.	SquirrelMail 'viewcert.php' Remote Code Execution	High	iDEFENSE Security Ad February 7, 2005
SquirrelMail Development Team SquirrelMail Vacation Plugin 0.14 -1.2rc2, 0.15 -1.43a	Two vulnerabilities exists in the 'ftpfile' program due to insufficient input validation, which could let a remote malicious user execute arbitrary commands with root privileges or obtain sensitive information. **Upgrades available at:** **http://www.squirrelmail.org/countdl.php?fileurl=http%3A%2F%2Fwww.squirrelmail.org%2Fplugins%2Fvacation_local-1.0-1.4.tar.gz** Proofs of Concept exploits scripts have been published.	SquirrelMail Vacation Plugin 'FTPFile' Input Validation	Medium/ High High if arbitrary code can be executed)	LSS Security Advisory, LSS-2005-01-03, Janu 2005 **SecurityFocus, Febru 2005**

SquirrelMail Development Team SquirrelMail 1.2.6	A vulnerability exists in 'src/webmail.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/squirrelmail_1.2.6-2_all.deb Currently we are not aware of any exploits for this vulnerability.	SquirrelMail Remote Code Execution CVE Name: CAN-2005-0152	High	Debian Security Adviso 662-1, February 1, 200
SuSE SuSE Linux Open-Xchange 4.1	A path traversal vulnerability exists, which could let a remote malicious user obtain sensitive information. SuSE: ftp://ftp.suse.com/pub/suse/ Currently we are not aware of any exploits for this vulnerability.	SuSE Linux Open-Xchange Path Traversal	Medium	SUSE Security Summa Report, SUSE-SR:2005 February 4, 2005
Todd Miller Sudo 1.5.6-1.5.9, 1.6-1.6.8	A vulnerability exists due to an error in the environment cleaning, which could let a malicious user execute arbitrary commands. Patch available at: http://www.courtesan.com/sudo/download.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sudo/ Debian: http://security.debian.org/pool/updates/main/s/sudo/ OpenPKG: ftp://ftp.openpkg.org/release/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	Sudo Restricted Command Execution Bypass	High	Secunia Advisory, SA13199, November 1 Mandrakelinux Security Advisory, MDKSA-2004 November 15, 2004 Trustix Secure Linux S Advisories, TSLSA-200 & 061, November 16 & 2004 Ubuntu Security Notice USN-28-1, November 1 Debian Security Adviso 596-1, November 24, 2 OpenPKG Security Adv OpenPKG-SA-2005.00 January 17, 2005 **Turbolinux Security Announcement, 2005 January 31, 2005**
University of Washington imap 2004b, 2004a, 2004, 2002b-2002e	A vulnerability exists due to a logic error in the Challenge-Response Authentication Mechanism with MD5 (CRAM-MD5) code, which could let a remote malicious user bypass authentication. Update available at: ftp://ftp.cac.washington.edu/mail/imap-2004b.tar.Z **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-02.xml** **Mandrake:**	University Of Washington IMAP Server CRAM-MD5 Remote Authentication Bypass	Medium	US-CERT Vulnerability VU#702777, January 2 **Gentoo Linux Securit Advisory, GLSA 2005 February 2, 2005** **Mandrakelinux Securi Update Advisory, MDKSA-2005:026, Feb 2005**

	http://www.mandrakesecure.net/ en/ftp.php Currently we are not aware of any exploits for this vulnerability.			
VIM Development Group VIM 6.0-6.2, 6.3.011, 6.3.025, 6.3 .030, 6.3.044, 6.3 .045	Multiple vulnerabilities exist in 'tcltags' and 'vimspell.sh' due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/v/vim/ **Mandrake:** **http://www.mandrakesecure.net /en/ftp.php** There is no exploit required.	Vim Insecure Temporary File Creation CVE Name: CAN-2005-0069	Medium	Secunia Advisory, SA13841, January 13, Ubuntu Security Notice USN-61-1, January 18, **Mandrakelinux Securi Update Advisory, MDKSA-2005:026, Feb 2005**
Yukihiro Matsumoto Ruby 1.6, 1.8	A vulnerability exists in the CGI session management component due to the way temporary files are processed, which could let a malicious user obtain elevated privileges. Upgrades available at: http://security.debian.org /pool/updates/main/r/ruby/ Gentoo: http://security.gentoo.org/ glsa/glsa-200409-08.xml RedHat: http://rhn.redhat.com/errata/ RHSA-2004-441.html Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/2/ Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/3/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Ruby CGI Session Management Unsafe Temporary File CVE Name: CAN-2004-0755	Medium	Debian Security Adviso 537-1, August 16, 2004 Gentoo Linux Security Advisory, GLSA 20040 September 3, 2004 RedHat Security Advis RHSA-2004:441-18, Se 30, 2004 Fedora Update Notifica FEDORA-2004-264, Oc 15, 2004 Mandrakelinux Security Advisory, MDKSA-2004 November 8, 2004 Fedora Update Notifica FEDORA-2004-403, No 11, 2004 **Turbolinux Security Announcement, 2005 January 31, 2005**
Yusuf Motiwala Newsfetch 1.4, 1.21	A buffer overflow vulnerability exists in 'nntp.c' due to insecure sscanf calls, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Yusuf Motiwala Newsfetch SScanf Remote Buffer Overflow CVE Name: CAN-2005-0132	High	Securiteam, February 2

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
BXCP 0.2.9.7 and prior	An input verification vulnerability exists that may allow disclosure of sensitive information. Input passed to the 'show' parameter in 'index.php' isn't properly verified. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	BXCP 'show' Local File Inclusion	Medium	Secunia SA14141, February 7, 2005
Chipmunk Forum 1.x	Multiple vulnerabilities exist which could permit SQL injection attacks. Input passed to various scripts isn't properly validated. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Chipmunk Forum SQL Injection Vulnerabilities	High	Secunia SA14143, February 7, 2005
Cisco Cisco IPVC-3510-MCU, Cisco IPVC-3520-GW-2B, Cisco IPVC-3520-GW-4B, Cisco IPVC-3520-GW-2, Cisco IPVC-3520-GW-4V, Cisco IPVC-3520-GW-2B2V, Cisco IPVC-3525-GW-1P, Cisco IPVC-3530-VTA	A vulnerability exists in some Cisco videoconferencing products that could permit a remote malicious user to gain control of the system using common default SNMP community strings. Cisco has issued a workaround available at: http://www.cisco.com/public/technotes/cisco-sa-20050202-ipvc.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IP/VC Remote Access	High	Cisco Security Advisory 63894, February 2, 2005
Cisco Linksys PSUS4 firmware 6032	A vulnerability exists which can could permit a Denial of Service. The vulnerability is caused due to an error in the HTTP POST request parsing. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Cisco Linksys PSUS4 Denial of Service	Low	SecurityFocus, Bugtraq ID 12443, February 3, 2005
CMScore	Multiple vulnerabilities exist which could permit SQL injection attacks due to improper validation of input passed to the 'EntryID,' 'searchterm,' and 'username' parameters. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	CMScore Multiple SQL Injection Vulnerabilities	High	Secunia SA14142, February 7, 2005
GPL Claroline 1.5 - 1.5.3	An input validation vulnerability exists that could permit script insertion attacks. Input passed to the 'wantedCode,' 'faculte,' 'intitule,' 'languageCourse,' 'titulaires,' and 'email' parameters in 'add_course.php' is not properly	GPL Claroline Script Insertion	High	SecurityFocus, Bugtraq ID 12449, February 4, 2004

	validated. Apply patch for version 1.5.3: http://www.claroline.net/dlarea/claroline153fix01.zip Currently we are not aware of any exploits for this vulnerability.			
JShop E-Commerce JShop Server prior to 1.2.0	A vulnerability exists that could permit Cross-Site Scripting attacks. This is due to improper input validation in the 'xProd' and 'xSec' parameters in 'product.php.' Update to version 1.3.0: http://www.jshop.co.uk/ **A Proof of Concept exploit has been published.**	JShop Server Cross-Site Scripting	High	SystemSecure, SS#27012005, January 30, 2005 **SecurityFocus, Bugtraq ID 12403, January 31, 2005**
Miro International Mambo 4.5.1	A vulnerability exists that could permit a user to administrative privileges and access the database. Global variables are not properly protected. Apply patch for version 4.5 and 4.5.1: http://www.mamboportal.com/component/option,com_remository/Itemid,46/ Currently we are not aware of any exploits for this vulnerability.	Miro International Mambo Access	High	MamboPortal Notice, February 2, 2005
Mozilla Mozilla 1.7.5, Firefox 1.0	A spoofing vulnerability exists that could permit a malicious website to spoof the URL displayed in the address bar, SSL certificate, and status bar. This is due to an unintended result of the IDN (International Domain Name) implementation, which allows using international characters in domain names. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla / Firefox / Camino IDN Spoofing	Medium	Secunia SA14163, February 7, 2005
Mozilla Mozilla 1.7.3	A heap overflow vulnerability exists in the processing of NNTP URLs. A remote malicious user can execute arbitrary code on the target system. A remote user can create a specially crafted 'news://' URL that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The flaw resides in the *MSG_UnEscapeSearchUrl() function in 'nsNNTPProtocol.cpp'. The vendor has issued a fixed version (1.7.5), available at: http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-03.xml SGI: http://support.sgi.com/browse_request/linux_patches_by_os	Mozilla Buffer Overflow in Processing NNTP URLs CVE Name: CAN-2004-1316	High	iSEC Security ResearchAdvisory, December 29, 2004 Gentoo Linux Security Advisor, GLSA 200501-03, January 5, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 **HP Security Advisory, HPSBTU01114, February 4, 2005**

	SuSE: ftp://ftp.suse.com/pub/suse/ **HP:** **http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01114** A Proof of Concept exploit has been published.			

Multiple Vendors
Check Point Software FireWall-1 R55 HFA08 with SmartDefense; Internet Security Systems SiteProtector 2.0.4.561, 2.0 SP3; IronPort IronPort with Sophos AV Engine 3.88;
McAfee Webshield 3000 4.3.20;
TippingPoint Unity-One with Digital Vaccine 2.0.0.2070;
Trend Micro InterScan Messaging Security Suite 3.81, 5.5,
Trend Micro WebProtect 3.1
	A security vulnerability exists due to a failure to decode base64-encoded images in 'data' URIs, which could lead to a false sense of security.
	TippingPoint:
	https://tmc.tippingpoint.com/TMC
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200501-46.xml
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	There is no exploit required.
		Multiple Vendor Anti-Virus GatewayBase64 Encoded Image Decode Failure	Medium	Bugtraq, January 11, 2005
				SecurityFocus, January 18, 2005
				Gentoo Linux Security Advisory, GLSA 200501-46, January 31, 2005
				Mandrakelinux Security Update Advisory, MDKSA-2005:025, February 2, 2005

Multiple Vendors Debian Linux 3.0 spar, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.7	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the DICOM dissector; a remote Denial of Service vulnerability exists in the handling of RTP timestamps; a remote Denial of Service vulnerability exists in the HTTP dissector; and a remote Denial of Service vulnerability exists in the SMB dissector when a malicious user submits specially crafted SMB packets. Potentially these vulnerabilities may also allow the execution of arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200412-15.xml Conectiva: ftp://atualizacoes.conectiva.com.br/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-011.html** **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Multiple Denial of Service & Potential Code Execution Vulnerabilities CVE Names: CAN-2004-1139 CAN-2004-1140 CAN-2004-1141 CAN-2004-1142	Low/High (High if arbitrary code can be executed)	Ethereal Security Advisory, enpa-sa-00016, December 15, 2004 Conectiva Linux Security Announcement, CLA-2005:916, January 13, 2005 **RedHat Security Advisory, RHSA-2005:011-11, February 2, 2005** **SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005**
Opera Software Opera	A spoofing vulnerability exists that could permit a malicious website to spoof the URL displayed in the address bar, SSL certificate, and status bar. This is due to an unintended result of the IDN	Opera IDN Spoofing	Medium	SecurityTracker Alert ID: 1013096, February 7, 2005

	(International Domain Name) implementation, which allows using international characters in domain names. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.			
PEiD 0.x	A vulnerability exists due to a boundary error within the parsing of the PE (Portable Executable) import directory that could allow execution of arbitrary code. **Update available at: http://www.absolutelock.de/construction/files/releases/PEiD-0.93-20050130.zip** Currently we are not aware of any exploits for this vulnerability.	PEiD Buffer Overflow **CVE Name: CAN-2005-0115**	High	iDEFENSE Security Advisory, January 24, 2005 **SecurityFocus, January 31, 2005**
PHP-Fusion 4.01	An information disclosure vulnerability exists due to an error in 'forum_search.php' when handling multiple search words. This may disclose the subjects of posts in protected forums.rafted search query. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	PHP-Fusion 'forum_search.php' Information Disclosure	Medium	Secunia SA14090, February 2, 2005
Python SimpleXMLRPCServer 2.2 all versions, 2.3 prior to 2.3.5, 2.4	A vulnerability exists in the SimpleXMLRPCServer library module that could permit a remote malicious user to access internal module data, potentially executing arbitrary code. Python XML-RPC servers that use the register_instance() method to register an object without a _dispatch() method are affected. Patches for Python 2.2, 2.3, and 2.4, available at: http://python.org/security/PSF-2005-001/patch-2.2.txt (Python 2.2) http://python.org/security/PSF-2005-001/patch.txt (Python 2.3, 2.4) The vendor plans to issue fixed versions for 2.3.5, 2.4.1, 2.3.5, and 2.4.1. Debian: http://www.debian.org/security/2005/dsa-666 Currently we are not aware of any exploits for this vulnerability.	Python SimpleXMLRPCServer Remote Code CVE Name: CAN-2005-0089	High	Python Security Advisory: PSF-2005-001, February 3, 2005
QNX Software Systems Ltd. RTOS 2.4, 4.25, 6.1 .0, 6.2 .0 Update Patch A, 6.2 .0	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in '/usr/bin/pppoed,' which could let a malicious user execute arbitrary code; buffer overflow vulnerabilities exist in 'name,' 'en', 'upscript,' 'downscript,' 'retries,' 'timeout,' 'scriptdetach,' 'noscript,' 'nodetach,' 'remote_mac,' and 'local_mac' flags, which could let a malicious user execute arbitrary code; and a vulnerability exists because the $PATH variable	QNX PPPoEd Buffer Overflows	High	Securiteam, September 6, 2004 **US-CERT Vulnerability Note, VU#577566** **US-CERT Vulnerability Note,**

	can be modified to cause the daemon to execute arbitrary code. **No vendor patch available at time of publishing. Workaround available through US-CERT Vulnerability Notes.** Proof of Concept exploit has been published.			**VU#961686**
softtime LiteForum 2.1.1	A vulnerability exists that could permit a remote user to inject SQL commands. 'enter.php' does not properly validate user-supplied data in the password parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	softtime LiteForum 'enter.php' Input Validation	High	SecurityTracker Alert ID: 1013084, February 4, 2005
Squid-cache.org Squid 2.5	A vulnerability exists that could permit a remote malicious user to send multiple Content-length headers with special HTTP requests to corrupt the cache on the Squid server. A patch (squid-2.5.STABLE7-header_parsing.patch) is available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-header_parsing.patch Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000923 **Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200502-04.xml** **Debian: http://www.debian.org/security/2005/dsa-667** **Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-77-1** **SuSE: ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Squid Error in Parsing HTTP Headers CVE Name: CAN-2005-0175	Medium	SecurityTracker Alert ID, 1012992, January 25, 2005 **Gentoo GLSA 200502-04, February 2, 2005** **Debian Security Advisory DSA-667-1, February 4, 2005** **SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005** **US-CERT Vulnerability Notes, VU#924198 & VU#625878**
SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/squirrelmail/sm143a-xss.diff?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-25.xml	SquirrelMail Cross-Site Scripting CVE Name: CAN-2004-1036 CAN-2005-0104 CAN-2005-0152	High	Secunia Advisory, SA13155, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-25, November 17, 2004 Fedora Update Notifications, FEDORA-2004-471 & 472, November 28, 2004

	Conectiva: ftp://atualizacoes.conectiva.com.br/9 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Apple: http://www.apple.com/support/downloads/ SuSE: ftp://ftp.suse.com/pub/suse/ **Debian:** **http://www.debian.org/security/2005/dsa-662** An exploit script is not required.			Conectiva Linux Security Announcement, CLA-2004:905, December 2, 2004 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 **Debian DSA-662-1, February 1, 2005**
Sun Microsystems, Inc. Sun Java JRE 1.3.x, 1.4.x, Sun Java SDK 1.3.x, 1.4.x; Conectiva Linux 10.0; Gentoo Linux; HP HP-UX B.11.23, B.11.22, B.11.11, B.11.00, HP Java SDK/RTE for HP-UX PA-RISC 1.3, HP Java SDK/RTE for HP-UX PA-RISC 1.4; Symantec Gateway Security 5400 Series v2.0.1, v2.0, Enterprise Firewall v8.0	A vulnerability exists due to a design error because untrusted applets for some private and restricted classes used internally can create and transfer objects, which could let a remote malicious user turn off the Java security manager and disable the sandbox restrictions for untrusted applets. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1 Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-38.xml HP: http://www.hp.com/go/java Symantec: http://securityresponse.symantec.com/avcenter/security/Content/2005.01.04.html **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Sun Java Plug-in Sandbox Security Bypass CVE Name: CAN-2004-1029	Medium	Sun(sm) Alert Notification, 57591, November 22, 2004 US-CERT Vulnerability Note, VU#760344, November 23, 2004 Conectiva Linux Security Announcement, CLA-2004:900, November 26, 2004 Gentoo Linux Security Advisory, GLSA 200411-38, November 29, 2004 HP Security Bulletin, HPSBUX01100, December 1, 2004 Sun(sm) Alert Notification, 57591, January 6, 2005 (Updated) Symantec Security Response, SYM05-001, January 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 **SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005**

Turnkey Web Tools SunShop Shopping Cart 3.4 RC4	A Cross-Site Scripting vulnerability exists due to improper validation of input passed to the 'search' parameter in 'index.php.' No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Turnkey SunShop Shopping Cart Cross-Site Scripting	High	SystemSecure, SS#25012005, February 3, 2005
University of California (BSD License) PostgreSQL 7.x, 8.x	Multiple vulnerabilities exist that could permit malicious users to gain escalated privileges or execute arbitrary code. These vulnerabilities are due to an error in the 'LOAD' option, a missing permissions check, an error in 'contrib/intagg,' and a boundary error in the plpgsql cursor declaration. Update to version 8.0.1, 7.4.7, 7.3.9, or 7.2.7: http://wwwmaster.postgresql.org/download/mirrors-ftp **Ubuntu:** **http://www.ubuntulinux.org/support/documentation/usn/usn-71-1** **Debian:** **http://www.debian.org/security/2005/dsa-668** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-08.xml** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for these vulnerabilities.	University of California PostgreSQL Multiple Vulnerabilities CVE Name: **CAN-2005-0227**	Medium/ High (High if arbitrary code can be executed)	PostgreSQL Security Release, February 1, 2005 **Ubuntu Security Notice USN-71-1 February 01, 2005** **Debian Security Advisory DSA-668-1, February 4, 2005** **Gentoo GLSA 200502-08, February 7, 2005**
Ventia DeskNow Mail and Collaboration Server 2.5.12	A vulnerability exists that could permit a remote user to upload or delete files to arbitrary locations on the target server. The 'attachment.do' script and the 'file.do' script do not properly validate user-supplied input. A fixed version (2.5.14 and later) is available at: http://www.desknow.com/desknowmc/downloads.html Currently we are not aware of any exploits for this vulnerability.	Ventia DeskNow Mail and Collaboration Server File Upload and Deletion	Medium	SIG^2 Vulnerability Research Advisory, February 2, 2005
x-dev xGB	A vulnerability exists that could permit a remote user to gain administrative access to the guest book. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	x-dev xGB Remote Access	Medium	SecurityTracker Alert, 1013091, February 7, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
February 6, 2005	AdvancedSQLInjectionInOracleDatabases.zip	N/A	A presentation that explores new methods in exploiting SQL injection vulnerabilities that are inherent in Oracle Database.
February 6, 2005	nmbscan-1.2.4.tar.gz	N/A	NMB Scanner scans the shares of a SMB network, using the NMB and SMB protocols. I
February 6, 2005	r57lite211.txt r57lite211.pl	No	Exploits for the softtime LiteForum 'enter.php' Input Validation vulnerability.
February 6, 2005	x_osh.pl oshexploit.pl	No	Perl script that exploits the Mike Neuman OSH Command Line Buffer Overflow vulnerability.
February 5, 2005	amap-4.8.tar.gz	N/A	A next-generation scanning tool that allows you to identify the applications that are running on a specific port by connecting to the port(s) and sending trigger packets.
February 5, 2005	hydra-4.6-src.tar.gz	N/A	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more that includes SSL support, parallel scans, and is part of Nessus.
February 5, 2005	newspost.c	Yes	Exploit for the Newspost Remote Buffer Overflow vulnerability.
February 5, 2005	oyxin.py foxmailDoS.txt	No	Scripts that exploit the Foxmail 'MAIL FROM' :Remote Buffer Overflow vulnerability.
February 3, 2005	ngircd_fsexp.c	No	Script that exploits the ngIRCd Remote Format String vulnerability.
February 3, 2005	painkkeybof.zip	Yes	Proof of Concept exploit for the Painkiller Buffer Overflow Remote Denial of Service vulnerability.
February 3, 2005	tinyweb19DoS.pl	No	Exploit for the TinyWeb Server Remote CGI Script Disclosure vulnerability.
February 2, 2005	/LANChatPR[1666c]DoS-poc.zip	No	Script that exploits the LANChat Pro Remote Denial of Service vulnerability.
February 2, 2005	fl0w-s33ker-v1.4.pl	N/A	Simple perl script that can be used to track overflows.
February 2, 2005	flow-adj-paper_en.txt	N/A	Whitepaper that discusses the exploration of adjacent memory against strncpy().
February 2, 2005	savantOverflowExplot.txt savant_bof.pl savant-explo.pl savant31remote.txt	No	Exploits for the Savant Web Server Remote Buffer Overflow vulnerability.
February 1, 2005	eternaldos.pl	No	A Proof of Concept exploit for the Eternal Lines Web Server Remote Denial of Service vulnerability.
February 1, 2005	newPostBufferOverflowExploit.c	Yes	A Proof of Concept exploit for the Newspost Remote Buffer Overflow vulnerability.

[back to top]

Trends

- In a recent study released by the think tank Ponemon Institute, 69% of companies say data breaches were the result of either malicious employee activities or non-malicious employee error. For more information, see 'Insiders, Not Hackers, Are Main Cause Of Data Breaches: Survey' located at: http://www.networkingpipeline.com/showArticle.jhtml?articleID=59301819 .
- According to Websense Security Labs, scammers are taking advantage of recent news that Microsoft is asking users to verify that they have a legitimate copy of Windows. Email messages that have the spoofed address of security@microsoft.com and with the heading "Microsoft Windows Update" ask recipients to update and/or validate both the Windows' serial number and the customer's credit card information on a Web site. For more information, see 'Phishers Fake Message From Microsoft' located at: http://www.techweb.com/wire/security/59301315

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-D	Win32 Worm	Increase	December 2004
3	Netsky-Q	Win32 Worm	Increase	March 2004
4	Sober-I	Win32 Worm	Slight Decrease	November 2004
5	Zafi-B	Win32 Worm	Decrease	June 2004
6	Netsky-D	Win32 Worm	Return to Table	March 2004
7	Bagle.bj	Win32 Worm	New to Table	January 2005
8	Netsky-B	Win32 Worm	Increase	February 2004
9	Bagle.z	Win32 Worm	Return to Table	April 2004
10	Bagle-AU	Win32 Worm	Decrease	October 2004

Table Updated February 8, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **None to report.**

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type

Admincash.A	Trj/Admincash.A	Trojan
Downloader.ALQ	Trj/Downloader.ALQ	Trojan
Gaobot.CTX	W32/Gaobot.CTX.worm	Win32 Worm
PWSteal.Sagic.B		Trojan
QLowZones-10		Trojan
SymbOS/Cabir.q		Symbian OS Worm
Troj/Baley-A		Trojan
Troj/Chimo-A		Trojan
Troj/Shine-B		Trojan
Trojan.Comxt.B		Trojan
VBS.Redlof.B		Win32 Worm
W32.Bobax.N	W32/Bobax-H	Win32 Worm
W32.Dopbot		Win32 Worm
W32.Gaobot.CII		Win32 Worm
W32.Mydoom.AR@mm		Win32 Worm
W32.Wallz	Net-Worm.Win32.Small.b	Win32 Worm
W32/Agobot-PN	Backdoor.Win32.Agobot.gen	Win32 Worm
W32/Ahker-B	Email-Worm.Win32.Anker.a	Win32 Worm
W32/Bobax.worm	WORM_BOBAX.K	Win32 Worm
W32/Bobax-F		Win32 Worm
W32/Bobax-H	Email-Worm.Win32.Bobic.a	Win32 Worm
W32/Bropia-D	IM-Worm.Win32.Exir.a WORM_BROPIA.F W32/Bropia.worm.g W32/Bropia.worm.f W32/Rbot-VD Win32/Bropia.D!Worm Win32.Bropia.D	Win32 Worm
W32/Bropia-F	IM-Worm.Win32.Slanec.a W32.Bropia.L W32/Bropia-F W32/Bropia.worm W32/Bropia.worm.i Win32.Bropia.F Win32/Bropia.F!Worm WORM_BROPIA.G	Win32 Worm
W32/LegMir-Z	Worm.Win32.Viking.a PE_LOOKED.B	Win32 Worm
W32/MyDoom-AO	Email-Worm.Win32.Mydoom.ak	Win32 Worm
W32/Protorid-AB		Win32 Worm
W32/Rbot-SQ	WORM_RBOT.AJD	Win32 Worm
W32/Rbot-UC		Win32 Worm
W32/Rbot-VC	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-VD		Win32 Worm
W32/Rbot-VM		Win32 Worm
W32/Rbot-VO	Backdoor.Win32.Rbot.gj W32/Sdbot.worm.gen.x	Win32 Worm
W32/Sdbot-UN	Backdoor.Win32.SdBot.us W32/Sdbot.BSD WORM_SDBOT.AMS	Win32 Worm
W32/Sober-J	Email-Worm.Win32.Sober.j Reblin	Win32 Worm

W32/Traxg-C	BKDR_MYWOMAN.A	Win32 Worm
Win32.Netmesser.A	AdClicker-BM TROJ_NETMESS.A Win32/Netmesser.A!Trojan	Trojan
Win32.Rbot.BPB	Backdoor.Win32.Rbot.hp W32/Rbot-VM W32/Sdbot.worm.gen.t Win32/Rbot.114688!Worm WORM_BROPIA.G	Win32 Worm
WORM_AGOBOT.AJC		Win32 Worm
WORM_BROPIA.F	Bropia.E Bropia.F IM-Worm.Win32.Exir.a W32.Bropia.E W32.Bropia.J W32/Bropia.E.worm W32/Bropia.F W32/Bropia.worm.g Win32.Bropia.E Win32.Rbot.BOM	
WORM_CISUM.A		Win32 Worm
WORM_MYDOOM.AE		Win32 Worm
WORM_MYDOOM.AF	I-Worm.Mydoom.ab I-Worm.Win32.Swash.31744 I-Worm/Swash.A W32.Mydoom.AG@mm W32/MyDoom-AG W32/Swash.A.worm Win32.Mydoom.AE Win32/Swash.A@mm Win32/Swash.D@mm Worm/MyDoom.AE WORM_SWASH.A	Win32 Worm
WORM_MYDOOM.AW	Win32/Mydoom.Variant!Worm	Win32 Worm
WORM_MYDOOM.AX	Win32/Mydoom.Variant!Worm	Win32 Worm
WORM_MYDOOM.AY	W32/MyDoom-AO Win32/Mydoom.Variant!Worm	Win32 Worm
WORM_RBOT.ALJ		Win32 Worm

[back to top]

Last updated February 09, 2005